



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/656,858	09/05/2003	Sonia Reed	016222-012810US	8576
20350	7590	09/19/2006		
TOWNSEND AND TOWNSEND AND CREW, LLP TWO EMBARCADERO CENTER EIGHTH FLOOR SAN FRANCISCO, CA 94111-3834			EXAMINER DWIVEDI, MAHESH H	
			ART UNIT 2168	PAPER NUMBER

DATE MAILED: 09/19/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/656,858	REED ET AL.	
	Examiner	Art Unit	
	Mahesh H. Dwivedi	2168	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 26 June 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,2,4-14,16-21,23-33,35-40,42-52 and 54-57 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,2,4-14,16-21,23-33,35-40,42-52 and 54-57 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 02 February 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>6/26/2006</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statements (IDS) submitted on 12/06/2003, 12/23/2003, and 6/26/2006 have been received, entered into the record, and considered. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Response to Amendment

2. Receipt of Applicant's Amendment, filed on 06/26/2006, is acknowledged. The amendment includes the cancellation of claims 3, 15, 22, 34, 41, and 53, and amending claims 1, 13, 18, 20, 32, 37, 39, and 56, and amending the specification.

Claim Objections

3. Claims 32, 37, and 56 are objected to because of the following informalities: The amendment received on 06/26/2006 stated that the aforementioned claims were in original form, but there are clearly amendments made to each claim. The examiner suggests that applicant replace "**original**" with "**currently amended**" in each of the aforementioned claims. Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

Art Unit: 2168

invention was made to a person having ordinary skill in the art to which said subject matter pertains.

Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

5. Claims 1-2, 4-14, 16-17, 19-21, 23-28, 30-33, 35-36, 38-40, 42-52, 54-55, and 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Deo et al.** (U.S. Patent 6,970,891) and in view of **Carlisle et al.** (U.S. Patent 5,649,118).

6. Regarding claim 1, **Deo** teaches a system comprising:

A) a client having a plurality of applications residing thereon (Column 3, lines 44-54);

and

B) a secure token having a storage architecture (Column 6, lines 27-34), wherein the storage architecture includes:

C) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure

2)

Art Unit: 2168

D) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2); and

E) one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

F) wherein the one or more attributes permit a first application to access after a first access condition is satisfied (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

G) wherein the one or more attributes permit a second application to access after a second access condition is satisfied (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

H) wherein the first access condition is different from the second access condition (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

The examiner notes that **Deo** teaches “**a client having a plurality of applications residing thereon**” as “The volatile files 122 make it possible for multiple resident applications 112, as well as nonresident applications 116 that are downloaded for a particular sessions, to share the same data in volatile memory 106 (assuming the applications are authorized)” (Column 3, lines 49-54). The examiner further notes that **Deo** teaches “**a secure token having a storage architecture**” as “With this architecture, volatile data kept in volatile memory is no longer bound to a single

Art Unit: 2168

application, but can be accessed by multiple applications" (Column 6, lines 27-29). The examiner further notes that Deo teaches **"wherein the one or more attributes are used to control access by the plurality of applications"** as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Deo teaches **"one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications"** as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Deo teaches **"wherein the one or more attributes permit a first application to access after a first access condition is satisfied"** as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further

Art Unit: 2168

notes that Deo teaches “**wherein the one or more attributes permit a second application to access after a second access condition is satisfied**” as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that Deo teaches “**wherein the first access condition is different from the second access condition**” as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that Figure 2 of Deo clearly shows an ACL table 204 with differing permission levels (see 1 and 4). The examiner further notes that App1 and User1 have different access conditions as they have different ACL values.

Deo does not explicitly teach:

- C) a directory and one or more attributes associated with the directory;
- D, F,G) one or more cell groups under the directory each cell group having one or more associated attributes.

Carlisle, however, teaches “**a directory and one or more attributes associated with the directory**” as “Multi-user capability is provided by allowing Root to

Art Unit: 2168

create a subdirectory below the root directory...only in the "passwd" file" (Column 5, lines 20-30) and **"one or more cell groups under the directory each cell group having one or more associated attributes"** as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory...only in the "passwd" file" (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by Carlisle (Column 1, lines 59-62).

Regarding claims 2, 21, and 40, **Deo** further teaches a system, secure token, and method comprising:

A) wherein the one or more attributes permit access to one application and deny access to another application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

The examiner further notes that **Deo** teaches **"wherein the one or more attributes permit access to one application and deny access to another application"** as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have

Art Unit: 2168

access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Figure 2 of **Deo** clearly shows an ACL table 204 with differing permission levels (see 1 and 4).

Deo does not explicitly teach:

A) associated with the directory.

Carlisle, however, teaches "**associated with the directory**" as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory...only in the "passwd" file" (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by Carlisle (Column 1, lines 59-62).

Regarding claims 4, 23, and 42, **Deo** further teaches a system, secure token, and method comprising:

A) wherein the one or more attributes associated with the cell permit access to that cell by one application and deny access to that cell to another application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44).

The examiner further notes that **Deo** teaches "**wherein the one or more attributes associated with the cell permit access to that cell by one application and deny access to that cell to another application**" as "an access control list (ACL)

Art Unit: 2168

can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42).

Regarding claims 5, 24, and 43 **Deo** further teaches a system, secure token, and method comprising:

A) wherein one or more additional cell groups are added to the directory subsequent to issuance of the secure token to a token holder (Column 7, lines 55-67).

The examiner further notes that **Deo** teaches “**wherein one or more additional cell groups are added to the directory subsequent to issuance of the secure token to a token holder**” as “ScwCreateDir Creates a directory with the given access control list (ACL) file” (Column 7, lines 57-58)

Regarding claims 6, 25, and 44, **Deo** does not explicitly teach a system, secure token, and method comprising:

A) wherein ownership of one of the one or more cell groups is determined subsequent to issuance of the secure token to a token holder.

Carlisle, however, teaches “**wherein ownership of one of the one or more cell groups is determined subsequent to issuance of the secure token to a token**

Art Unit: 2168

holder" as "First, O, controls the establishment of a service provider's directory"
(Column 14, lines 63-64).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by Carlisle (Column 1, lines 59-62).

Regarding claims 7, 26, and 45, **Deo** does not explicitly teach a system, secure token, and method comprising:

A) wherein ownership of one of the one or more cell groups is modified subsequent to issuance of the secure token to a token holder.

Carlisle, however, teaches "**wherein ownership of one of the one or more cell groups is modified subsequent to issuance of the secure token to a token holder**" as "First, O, controls the establishment of a service provider's directory...through the operating system's design, O can control the amount of memory that each service provider has access to, and thus can control the number of service providers that can "coexist" on a smart card"" (Column 14, lines 63-67-Column 15, lines 1-10).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical

Art Unit: 2168

levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by Carlisle (Column 1, lines 59-62).

Regarding claims 8, 27, and 46, **Deo** further teaches a system, secure token, and method comprising:

A) wherein one or more additional cells are added to a cell group subsequent to issuance of the secure token to a token holder (Column 6, lines 62-67).

The examiner notes that Deo teaches **“wherein one or more additional cells are added to a cell group subsequent to issuance of the secure token to a token holder”** as “At block 304, in response to a request from an authorized application to create or open a file, the file system 118 creates or opens a file and obtains a handle to that file” (Column 6, lines 62-67).

Regarding claims 9, 28, and 47, **Deo** further teaches a system, secure token, and method comprising:

A) wherein the one or more attributes associated are modified in terms of permitting or denying access by the plurality of applications (Column 4, lines 37-44).

The examiner notes that **Deo** teaches **“wherein the one or more attributes associated with the directory are modified in terms of permitting or denying access to the directory by the plurality of applications”** as “the file system includes an ACL (access control list) that performs the security function of determining which users and/or applications have access to which files” (Column 4, lines 37-44).

Art Unit: 2168

Deo does not explicitly teach:

A) with the directory.

Carlisle, however, teaches “**with the directory**” as “Multi-user capability is provided by allowing Root to create a subdirectory below the root directory... only in the “passwd” file” (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle’s** would have allowed **Deo’s** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by Carlisle (Column 1, lines 59-62).

Regarding claims 10 and 48, **Deo** further teaches a system and method comprising:

A) wherein the one or more attributes associated are modified in terms of permitting or denying access by the plurality of applications (Column 4, lines 37-44).

The examiner notes that **Deo** teaches “**wherein the one or more attributes associated with a cell group are modified in terms of permitting or denying access to that cell group by the plurality of applications**” as “the file system includes an ACL (access control list) that performs the security function of determining which users and/or applications have access to which files” (Column 4, lines 37-44).

Deo does not explicitly teach:

A) with the cell group.

Carlisle, however, teaches **“with the cell group”** as “Multi-user capability is provided by allowing Root to create a subdirectory below the root directory...only in the “passwd” file” (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle’s** would have allowed **Deo’s** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by Carlisle (Column 1, lines 59-62).

Regarding claims 11, 30, and 49, **Deo** further teaches a system, secure token, and method comprising:

A) wherein the one or more attributes associated with the cell are modified in terms of permitting or denying access to that cell by the plurality of applications (Column 4, lines 37-44).

The examiner notes that **Deo** teaches **“wherein the one or more attributes associated with the cell are modified in terms of permitting or denying access to that cell by the plurality of applications”** as “the file system includes an ACL (access control list) that performs the security function of determining which users and/or applications have access to which files” (Column 4, lines 37-44).

Regarding claims 12, 31, and 50, **Deo** further teaches a system, secure token, and method comprising:

Art Unit: 2168

A) wherein the one or more attributes associated with a cell further control operations on contents of that cell by the plurality of applications (Column 4, lines 37-44):

The examiner notes that **Deo** teaches “**wherein the one or more attributes associated with a cell further control operations on contents of that cell by the plurality of applications**” as “the file system includes an ACL (access control list) that performs the security function of determining which users and/or applications have access to which files” (Column 4, lines 37-44).

Regarding claim 13, **Deo** teaches a system comprising:

A) a client having a plurality of applications residing thereon (Column 3, lines 44-54);

and

B) a secure token having a storage architecture (Column 6, lines 27-34), wherein the storage architecture includes:

C) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure

2)

D) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure

2); and

E) one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control

Art Unit: 2168

access to that cell by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

F) wherein the one or more attributes associated with the cell permit a first set of operations on the contents of that cell by a first application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

G) wherein the one or more attributes associated with the cell permit a second set of operations on the contents of that cell by a second application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

H) wherein the first access condition is different from the second access condition (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

The examiner notes that **Deo** teaches **“a client having a plurality of applications residing thereon”** as “The volatile files 122 make it possible for multiple resident applications 112, as well as nonresident applications 116 that are downloaded for a particular sessions, to share the same data in volatile memory 106 (assuming the applications are authorized)” (Column 3, lines 49-54). The examiner further notes that **Deo** teaches **“a secure token having a storage architecture”** as “With this architecture, volatile data kept in volatile memory is no longer bound to a single application, but can be accessed by multiple applications” (Column 6, lines 27-29). The examiner further notes that **Deo** teaches **“wherein the one or more attributes are used to control access by the plurality of applications”** as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes

Art Unit: 2168

an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Deo teaches **"one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications"** as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Deo teaches **"wherein the one or more attributes associated with the cell permit a first set of operations on the contents of that cell by a first application"** as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Deo teaches **"wherein the one or more attributes associated with the cell permit a second set of operations on the contents of that cell by a second application"** as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL

Art Unit: 2168

(access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches "**wherein the first access condition is different from the second access condition**" as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Figure 2 of **Deo** clearly shows an ACL table 204 with differing permission levels (see 1 and 4). The examiner further notes that App1 and User1 have different access conditions as they have different ACL values.

Deo does not explicitly teach:

- C) a directory and one or more attributes associated with the directory;
- D) one or more cell groups under the directory each cell group having one or more associated attributes.

Carlisle, however, teaches "**a directory and one or more attributes associated with the directory**" as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory...only in the "passwd" file" (Column 5, lines 20-30) and "**one or more cell groups under the directory each cell group having one or more associated attributes**" as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory...only in the "passwd" file" (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by Carlisle (Column 1, lines 59-62).

Regarding claims 14, 33, and 52, **Deo** further teaches a system, secure token, and method comprising:

- A) wherein the one or more attributes permit a first set of operations by a first application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);
- B) wherein the one or more attributes permit a second set of by a second application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);
- C) wherein the first access condition is different from the second access condition (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

The examiner notes that **Deo** teaches "**wherein the one or more attributes permit a first set of operations by a first application**" as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches "**wherein the one or more**

attributes permit a second set of by a second application" as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches "**wherein the first access condition is different from the second access condition**" as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Figure 2 of **Deo** clearly shows an ACL table 204 with differing permission levels (see 1 and 4). The examiner further notes that App1 and User1 have different access conditions as they have different ACL values.

Deo does not explicitly teach:

A, B) associated with the directory.

Carlisle, however, teaches "**associated with the directory**" as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory...only in the "passwd" file" (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical

Art Unit: 2168

levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by Carlisle (Column 1, lines 59-62).

Regarding claims 16, 35, 51, and 54, **Deo** further teaches a system comprising:

- A) wherein the one or more attributes associated with the cell permit a first set of operations on the contents of that cell by a first application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);
- B) wherein the one or more attributes associated with the cell permit a second set of operations on the contents of that cell by a second application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);
- C) wherein the first access condition is different from the second access condition (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

The examiner notes that **Deo** teaches “**wherein the one or more attributes associated with the cell permit a first set of operations on the contents of that cell by a first application**” as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that **Deo** teaches “**wherein the one or more attributes associated with the cell permit a second set of operations on the contents of that cell by a second application**” as “an access control list (ACL) can be associated...gain access to and

Art Unit: 2168

perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches "**wherein the first access condition is different from the second access condition**" as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Figure 2 of **Deo** clearly shows an ACL table 204 with differing permission levels (see 1 and 4). The examiner further notes that App1 and User1 have different access conditions as they have different ACL values.

Regarding claims 17, 36, and 55, **Deo** further teaches a system, secure token, and method comprising:

A) wherein the secure token is a smart card (Column 1, lines 6-8).

The examiner notes that **Deo** teaches "**wherein the secure token is a smart card**" as "This invention relates to integrated circuit (IC modules, such as smart cards" (Column 1, lines 6-7).

Regarding claims 19, 38, and 57, **Deo** further teaches a system, secure token, and method comprising:

A) wherein the secure token is a static or native smart card (Column 3, lines 44-54).

The examiner notes that **Deo** teaches “**wherein the secure token is a static or native smart card**” as “The operating system 114 includes a file system 118 that manages files stored on the smart card” (Column 3, lines 44-45).

Regarding claim 20, **Deo** teaches a secure token comprising:

A) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2)

B) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2); and

C) one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

D) wherein the one or more attributes permit a first application to access after a first access condition is satisfied (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

Art Unit: 2168

E) wherein the one or more attributes permit a second application to access after a second access condition is satisfied (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

F) wherein the first access condition is different from the second access condition (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

The examiner notes that **Deo** teaches “**wherein the one or more attributes are used to control access by the plurality of applications**” as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that **Deo** teaches “**one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications**” as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that **Deo** teaches “**wherein the one or more attributes permit a first application to access after a first access condition is satisfied**” as “an access control list (ACL) can be associated...gain access to and

Art Unit: 2168

perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Deo teaches "**wherein the one or more attributes permit a second application to access after a second access condition is satisfied**" as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Deo teaches "**wherein the first access condition is different from the second access condition**" as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Figure 2 of Deo clearly shows an ACL table 204 with differing permission levels (see 1 and 4). The examiner further notes that App1 and User1 have different access conditions as they have different ACL values.

Deo does not explicitly teach:

A) a directory and one or more attributes associated with the directory;

Art Unit: 2168

B, D, E) one or more cell groups under the directory each cell group having one or more associated attributes.

Carlisle, however, teaches **“a directory and one or more attributes associated with the directory”** as “Multi-user capability is provided by allowing Root to create a subdirectory below the root directory...only in the “passwd” file” (Column 5, lines 20-30) and **“one or more cell groups under the directory each cell group having one or more associated attributes”** as “Multi-user capability is provided by allowing Root to create a subdirectory below the root directory...only in the “passwd” file” (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle’s** would have allowed **Deo’s** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by Carlisle (Column 1, lines 59-62)..

Regarding claim 32, **Deo** teaches a secure token comprising:

A) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure

2)

B) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure

2); and

Art Unit: 2168

C) one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

D) wherein the one or more attributes associated with the cell permit a first set of operations on the contents of that cell by a first application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

E) wherein the one or more attributes associated with the cell permit a second set of operations on the contents of that cell by a second application (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

F) wherein the first access condition is different from the second access condition (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

The examiner notes that **Deo** teaches “a client having a plurality of applications residing thereon” as “The volatile files 122 make it possible for multiple resident applications 112, as well as nonresident applications 116 that are downloaded for a particular sessions, to share the same data in volatile memory 106 (assuming the applications are authorized)” (Column 3, lines 49-54). The examiner further notes that **Deo** teaches “a secure token having a storage architecture” as “With this architecture, volatile data kept in volatile memory is no longer bound to a single application, but can be accessed by multiple applications” (Column 6, lines 27-29). The examiner further notes that **Deo** teaches “wherein the one or more attributes are used to control access by the plurality of applications” as “an access control list

Art Unit: 2168

(ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that Deo teaches **“one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications”** as “an access control list (ACL) can be

associated...gain access to and perform file operations on the volatile files 122”

(Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that Deo teaches **“wherein the one or more attributes associated with the cell permit a first set of operations on the contents of that cell by a first application”** as “an access control list (ACL) can be

associated...gain access to and perform file operations on the volatile files 122”

(Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that Deo teaches **“wherein the one or more attributes associated with the cell permit a second set of operations on the contents of that cell by a second application”** as “an access control list (ACL) can be

Art Unit: 2168

associated...gain access to and perform file operations on the volatile files 122"

(Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches "**wherein the first access condition is different from the second access condition**" as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Figure 2 of **Deo** clearly shows an ACL table 204 with differing permission levels (see 1 and 4). The examiner further notes that App1 and User1 have different access conditions as they have different ACL values.

Deo does not explicitly teach:

- A) a directory and one or more attributes associated with the directory;
- B) one or more cell groups under the directory each cell group having one or more associated attributes.

Carlisle, however, teaches "**a directory and one or more attributes associated with the directory**" as "Multi-user capability is provided by allowing Root to create a subdirectory below the root directory...only in the "passwd" file" (Column 5, lines 20-30) and "**one or more cell groups under the directory each cell group having one or more associated attributes**" as "Multi-user capability is provided by

Art Unit: 2168

allowing Root to create a subdirectory below the root directory...only in the "passwd" file" (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle's** would have allowed **Deo's** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by Carlisle (Column 1, lines 59-62).

Regarding claim 39, **Deo** teaches a method comprising:

- A) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2)
- B) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2); and
- C) one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).
- D) wherein the one or more attributes permit a first application to access after a first access condition is satisfied (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

Art Unit: 2168

E) wherein the one or more attributes permit a second application to access after a second access condition is satisfied (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2);

F) wherein the first access condition is different from the second access condition (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

The examiner notes that **Deo** teaches “**wherein the one or more attributes are used to control access by the plurality of applications**” as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that **Deo** teaches “**one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications**” as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that **Deo** teaches “**wherein the one or more attributes permit a first application to access after a first access condition is satisfied**” as “an access control list (ACL) can be associated...gain access to and

Art Unit: 2168

perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches "wherein the one or more attributes permit a second application to access after a second access condition is satisfied" as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that **Deo** teaches "wherein the first access condition is different from the second access condition" as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Figure 2 of **Deo** clearly shows an ACL table 204 with differing permission levels (see 1 and 4). The examiner further notes that App1 and User1 have different access conditions as they have different ACL values.

Deo does not explicitly teach:

A) providing a directory and one or more attributes associated with the directory;

Art Unit: 2168

B, D, and E) providing one or more cell groups under the directory each cell group having one or more associated attributes.

Carlisle, however, teaches “**providing a directory and one or more attributes associated with the directory**” as “Multi-user capability is provided by allowing Root to create a subdirectory below the root directory...only in the “passwd” file” (Column 5, lines 20-30) and “**providing one or more cell groups under the directory each cell group having one or more associated attributes**” as “Multi-user capability is provided by allowing Root to create a subdirectory below the root directory...only in the “passwd” file” (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle’s** would have allowed **Deo’s** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by **Carlisle** (Column 1, lines 59-62).

7. Claims 18, 37, and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Deo et al.** (U.S. Patent 6,970,891) and in view of **Carlisle et al.** (U.S. Patent 5,649,118) as applied to claims 1-2, 4-14, 16-17, 19-21, 23-28, 30-33, 35-36, 38-40, 42-52, 54-55, and 57 and further in view of **Brittenham et al.** (U.S. Patent 6,880,084)

8. Regarding claim 18, **Deo** teaches a system comprising:

Art Unit: 2168

A) a client having a plurality of applications residing thereon (Column 3, lines 44-54);

and

B) a secure token having a storage architecture (Column 6, lines 27-34), wherein the storage architecture includes:

C) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure

2)

D) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure

2); and

E) one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

The examiner notes that Deo teaches “a client having a plurality of applications residing thereon” as “The volatile files 122 make it possible for multiple resident applications 112, as well as nonresident applications 116 that are downloaded for a particular sessions, to share the same data in volatile memory 106 (assuming the applications are authorized)” (Column 3, lines 49-54). The examiner further notes that Deo teaches “a secure token having a storage architecture” as “With this architecture, volatile data kept in volatile memory is no longer bound to a single application, but can be accessed by multiple applications” (Column 6, lines 27-29). The

Art Unit: 2168

examiner further notes that Deo teaches **“wherein the one or more attributes are used to control access by the plurality of applications”** as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that Deo teaches **“one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications”** as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that Deo teaches **“wherein the one or more attributes permit a first application to access after a first access condition is satisfied”** as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that Deo teaches **“wherein the one or more attributes permit a second**

application to access after a second access condition is satisfied” as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that **Deo** teaches “**wherein the first access condition is different from the second access condition**” as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that Figure 2 of **Deo** clearly shows an ACL table 204 with differing permission levels (see 1 and 4). The examiner further notes that App1 and User1 have different access conditions as they have different ACL values.

Deo does not explicitly teach:

- C) a directory and one or more attributes associated with the directory;
- D) one or more cell groups under the directory each cell group having one or more associated attributes.

Carlisle, however, teaches “**a directory and one or more attributes associated with the directory**” as “Multi-user capability is provided by allowing Root to create a subdirectory below the root directory...only in the “passwd” file” (Column 5,

Art Unit: 2168

lines 20-30) and “one or more cell groups under the directory each cell group having one or more associated attributes” as “Multi-user capability is provided by allowing Root to create a subdirectory below the root directory... only in the “passwd” file” (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle’s** would have allowed **Deo’s** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by Carlisle (Column 1, lines 59-62).

Deo and **Carlisle** do not explicitly teach:

F) wherein the smart card is an open platform smart card.

Brittenham, however, teaches **“wherein the smart card is an open platform smart card”** as “embodiments of the present invention may support Java Card (with Open Platform support), multi-application operating system for smart cards (MULTOS) or Smart Card for Windows” (Column 7, lines 60-64).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Brittenham’s** would have allowed **Deo’s** and **Carlisle’s** to provide for the coordinating of the efforts of multiple enterprises on a single smart card to enable a hierarchy, as noted by **Brittenham** (Column 1, lines 50-54).

Regarding claim 37, **Deo** teaches a secure token comprising:

A) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure

2)

B) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure

2); and

C) one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

The examiner notes that Deo teaches **“wherein the one or more attributes are used to control access by the plurality of applications”** as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that Deo teaches **“one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications”** as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL

Art Unit: 2168

(access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Deo teaches "**wherein the one or more attributes permit a first application to access after a first access condition is satisfied**" as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Deo teaches "**wherein the one or more attributes permit a second application to access after a second access condition is satisfied**" as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Deo teaches "**wherein the first access condition is different from the second access condition**" as "an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122" (Column 3, lines 66-67-Column 4, lines 1-5) and "The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like" (Column 4, lines 37-42). The examiner further notes that Figure 2 of Deo

Art Unit: 2168

clearly shows an ACL table 204 with differing permission levels (see 1 and 4). The examiner further notes that App1 and User1 have different access conditions as they have different ACL values.

Deo does not explicitly teach:

- A) a directory and one or more attributes associated with the directory;
- B) one or more cell groups under the directory each cell group having one or more associated attributes.

Carlisle, however, teaches “a directory and one or more attributes associated with the directory” as “Multi-user capability is provided by allowing Root to create a subdirectory below the root directory...only in the “passwd” file” (Column 5, lines 20-30) and “one or more cell groups under the directory each cell group having one or more associated attributes” as “Multi-user capability is provided by allowing Root to create a subdirectory below the root directory...only in the “passwd” file” (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle’s** would have allowed **Deo’s** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by Carlisle (Column 1, lines 59-62).

Deo and **Carlisle** do not explicitly teach:

- D) wherein the smart card is an open platform smart card.

Brittenham, however, teaches “**wherein the smart card is an open platform smart card**” as “embodiments of the present invention may support Java Card (with Open Platform support), multi-application operating system for smart cards (MULTOS) or Smart Card for Windows” (Column 7, lines 60-64).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Brittenham’s** would have allowed **Deo’s** and **Carlisle’s** to provide for the coordinating of the efforts of multiple enterprises on a single smart card to enable a hierarchy, as noted by **Brittenham** (Column 1, lines 50-54).

Regarding claim 56, **Deo** teaches a method comprising:

- A) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2)
- B) wherein the one or more attributes are used to control access by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2); and
- C) one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications (Column 3, lines 64-67-Column 4, lines 1-6, Column 4, lines 37-44, Figure 2).

The examiner notes that Deo teaches **“wherein the one or more attributes are used to control access by the plurality of applications”** as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that Deo teaches **“one or more cells under each cell group, each cell having one or more associated attributes, wherein the one or more attributes associated with a cell are used to control access to that cell by the plurality of applications”** as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that Deo teaches **“wherein the one or more attributes permit a first application to access after a first access condition is satisfied”** as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that Deo teaches **“wherein the one or more attributes permit a second**

application to access after a second access condition is satisfied as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that Deo teaches “**wherein the first access condition is different from the second access condition**” as “an access control list (ACL) can be associated...gain access to and perform file operations on the volatile files 122” (Column 3, lines 66-67-Column 4, lines 1-5) and “The file system 118 includes an ACL (access control list) table 204 that performs the security function of determining which users and/or applications have access to which files...and the like” (Column 4, lines 37-42). The examiner further notes that Figure 2 of Deo clearly shows an ACL table 204 with differing permission levels (see 1 and 4). The examiner further notes that App1 and User1 have different access conditions as they have different ACL values.

Deo does not explicitly teach:

- A) providing a directory and one or more attributes associated with the directory;
- B) providing one or more cell groups under the directory each cell group having one or more associated attributes.

Carlisle, however, teaches “**providing a directory and one or more attributes associated with the directory**” as “Multi-user capability is provided by allowing Root to create a subdirectory below the root directory...only in the “passwd” file” (Column 5,

Art Unit: 2168

lines 20-30) and “providing one or more cell groups under the directory each cell group having one or more associated attributes” as “Multi-user capability is provided by allowing Root to create a subdirectory below the root directory...only in the “passwd” file” (Column 5, lines 20-30).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Carlisle’s** would have allowed **Deo’s** to provide for access control at higher hierarchical levels including subfolders and folders in order to restrict access to some providers on a smart card, as noted by Carlisle (Column 1, lines 59-62).

Deo and **Carlisle** do not explicitly teach:

D) wherein the smart card is an open platform smart card.

Brittenham, however, teaches “**wherein the smart card is an open platform smart card**” as “embodiments of the present invention may support Java Card (with Open Platform support), multi-application operating system for smart cards (MULTOS) or Smart Card for Windows” (Column 7, lines 60-64).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of the cited references because teaching **Brittenham’s** would have allowed **Deo’s** and **Carlisle’s** to provide for the coordinating of the efforts of multiple enterprises on a single smart card to enable a hierarchy, as noted by **Brittenham** (Column 1, lines 50-54).

Response to Arguments

Art Unit: 2168

9. Applicant's arguments with respect to claims 1-2, 4-14, 16-21, 23-33, 35-40, 42-52, and 54-57 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent 6,199,762 issued to **Hohle** on 13 March 2001. The subject matter disclosed therein is pertinent to that of claims 1-2, 4-14, 16-21, 23-33, 35-40, 42-52, and 54-57 (e.g., methods to secure and use smart cards).

U.S. Patent 6,367,011 issued to **Lee et al.** on 02 April 2002. The subject matter disclosed therein is pertinent to that of claims 1-2, 4-14, 16-21, 23-33, 35-40, 42-52, and 54-57 (e.g., methods to secure and use smart cards).

U.S. Patent 5,682,027 issued to **Bertina et al.** on 28 October 1997. The subject matter disclosed therein is pertinent to that of claims 1-2, 4-14, 16-21, 23-33, 35-40, 42-52, and 54-57 (e.g., methods to secure and use smart cards).

U.S. Patent 6,481,632 issued to **Wentker et al.** on 19 November 2002. The subject matter disclosed therein is pertinent to that of claims 1-2, 4-14, 16-21, 23-33, 35-40, 42-52, and 54-57 (e.g., methods to secure and use smart cards).

Contact Information

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Mahesh Dwivedi whose telephone number is (571) 272-2731. The examiner can normally be reached on Monday to Friday 8:20 am – 4:40 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tim Vo can be reached (571) 272-3642. The fax number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Mahesh Dwivedi

Patent Examiner

Art Unit 2168



September 15, 2006



Leslie Wong